message from the board

Mid-Columbia Members,

I hope everyone is enjoying the cooler fall temperatures, or maybe these are winter temperatures?

Last month we gained a lot of information on how to keep your electronic devices safe and secure thanks to Eric Thomas, IT Security Engineer from Gesa Credit Union. Did you miss his presentation? We have added his slides onto our Chapter Website for your convenience. Did you know that you can also find monthly luncheon information, trainings, and past presentation slides on the website?

This month we are welcoming Tonya Hodge and Brandon Allison, both from Gesa, with their presentation on “Fighting Today’s Fraud”. Join us Thursday, October 17th at 11:30 at the Richland Public Library.

Have a great month and happy auditing!

Mid-Columbia Chapter Board Members

audit career center

Advance your internal audit career or strengthen your team with The IIA’s Audit Career Center resources.

upcoming webinars

Enhancing Internal Audit Effectiveness Through Core Principles
Members-only Webinar:
Tuesday, October 15, 2019
1:00 – 2:00 p.m. ET

DID YOU KNOW THAT THE IIA WEBSITE HAS A LARGE LIBRARY OF ONDEMAND COURSES AVAILABLE ON YOUR OWN TIME?

What do you call an accountant with an opinion?
Answer: An Auditor

2020 seminar details - save the date:

Did you attend our luncheon last year with Steve Hunt? We are excited to announce that he will be back to show us more excel tips in a one-day training seminar this spring! Keep checking back for updates as we finalize the details!
WHAT’S IN THE NEWS?
The Difference Between Operational Risk Management and Operational Resilience

John Thackeray
Founder and CEO of Risk Smart Inc.

Operational resilience is a set of techniques that allow people, processes and informational systems to adapt to changing patterns. In other words, it is the ability to alter operations in the face of changing business conditions. Operationally resilient enterprises have the competency to ramp up or slow down operations in a way that provides a competitive edge, and enables quick and local process modification.

A resilient enterprise is able to recover its key business services from a significant unplanned disruption, protecting its customers, shareholders and ultimately the integrity of the financial system. Operational resilience is about more than just protecting the resilience of systems — it also covers governance, strategy, business services, information security, change management, run processes and disaster recovery.
Operating environment

The operating environment for financial firms has changed significantly in recent years, with many adverse and material events becoming a near certainty. Regulators now want operational resilience to be something that boards and senior managers are directly engaged with and responsible for through governance and assurance models. As a result, regulators are keen on promoting the principles behind having an effective resilience program and its benefits for firms, customers and markets. In July 2018, the U.K.’s financial services regulators (The Bank of England, The Prudential Regulation Authority and Financial Conduct Authority) brought the concept of operational resilience into the limelight, with the publication of a joint discussion paper, Building the UK Financial Sector’s Operational Resilience.

The key requirements noted in the discussion paper include:

- **Governance**: The importance of operational resilience in the boardroom cannot be overstated. Accountabilities and responsibilities for senior management should be clearly defined and set against an unambiguous chain of command.
- **Business operating model**: The model must be properly understood, including key business services and the people, systems, processes and third parties that support them.
- **Risk appetite and tolerances**: Organizations should understand and be able to clearly articulate their operational risk appetite. This includes outlining impact tolerance for disruptions to key business services, through the lenses of impact to markets, consumers and business viability.
- **Planning and communications**: Organizations will need to have meaningful plans with emphasis placed on the performance of these plans. The plans should be supplemented by proposals for testing not only by the organizations themselves but in partnership with contributing stakeholders.
- **Culture**: When organizations emphasize operational resilience, there must also be a shift in mindset toward service continuity and a continuous improvement approach. By embedding a “resilience culture,” organizations reinforce and promote resilient and adaptive behaviors.

Operational offense

I suggest these five critical actions to support and evolve your organization’s approach to operational resilience.

1. **Identify your critical services**: Begin by documenting your business services and mapping them to the underlying technology (cloud infrastructure, data centers, applications, etc.) and business processes (disaster recovery, cyber-incident response plans, etc.).

2. **Understand impact tolerance**: Assess these underlying technologies and processes against Key Performance Indicators (KPIs) or Key Risk Indicators (KRIs). Use your assessment to create a risk score for each business service and review those scores against agreed-upon impact tolerances. Through the use of scenarios, you can estimate the extent of disruption to a business service that could be tolerated. Scenarios should be severe but plausible and assume that a failure of a system or process has occurred. This is where you decide your organization’s tolerance for disruption — the point at which disruption is no longer tolerable.

3. **Know your environment**: Use the assessment to develop a remediation plan that gives priority to the business services with the largest disparity between risk score and acceptable impact tolerance. Communicate your organization’s plan to regulators, ensuring that it’s aligned with their expectations. Once you have their buy-in, fund and execute the remediation plan. Afterward, you will reassess the business service for resilience. This should incorporate third parties, who are the second biggest root cause of operational outages after change management.
4. **Operationalize the program**: The operational resilience program must be able to evolve with the business as it changes. Understand what external or internal factors could change over time and what trends could impact the key business services identified, and adjust your resilience plans accordingly. An important step in this process is testing, which is also prioritized by the risk materiality of your organization’s key business services. Testing and simulating disruption events can advance your enterprise from informed assessments to demonstrated capabilities in the eyes of stakeholders and regulators.

5. **Robust and coherent reporting**: For boards and senior management, risk metrics and reporting provide an important insight into the effectiveness of the operational resilience program. Develop clear and transparent stakeholder communication plans. Having a robust communication policy and strategy is an essential part of any resilience program, using all forms of media and engaging with all stakeholders.

Essentially, operational resilience is an upgrade that moves operational risk management from passive to active. Operational resilience is the poor sibling of credit and market risk, but it has now stepped into the limelight. Like Cinderella, it needs an upscaling and upgrading of both resources and vision to make it happen. Given the number of pressing regulatory programs, it will be interesting to see how firms weave this requirement into their infrastructure and mindset.

*John Thackeray is the founder and CEO of Risk Smart Inc., a consulting firm that specializes in the writing of risk documentation. RiskSmartInc helps firms control their risks by bringing their documentation to life, so that the organization can live and breathe more soundly at night.*

---

**NEW CIA Exam Now Available:**

Adding the CIA credential to your resume will help you stand out and demonstrate that you are:

- A credible & trusted internal auditor
- A true expert who understands and can apply the Standards
- A stronger, more competent professional who is knowledgeable in organizational governance
- Committed to the profession of internal auditing and equipped for career-advancing opportunities
- Differentiated from your peers

Plus, CIAs earn an average of $38,000 more annually than those without a certification. Join the over 160,000 CIAs in 170+ countries awarded the designation that adds immeasurable distinction with only three letters

---

**FRAUD WATCH:**

- **10 Most Common Phone Scams to Look Out For**

---

**DID YOU KNOW?**

- One quarter of all the candy sold annually in the U.S. is purchased for Halloween.
- Pumpkin Spice has been a thing for 3,500 years; ancient nutmeg residue was found on ceramic pottery shards that they estimate to be 3,500 years old.
- Candy corn was invented in the 1880’s where over half of the American labor force were farmers; it was designed to appeal to the farmer’s children and originally called “Chicken Feed”.

---